FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1577572-000

Total Deleted Page(s) = 1
Page 25 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

b6
b7C

221

Memorandum

To : DIRECTOR, FBI

Date 3/24/93

From [redacted] T CANBERRA [redacted] (P)

~~SECRET~~

b3
b6
b7C
b7E

Subject: [redacted]

OO: SF

This communication is classified ~~"SECRET"~~ in its entirety.

Reference: Bureau teletype dated 3/22/93, captioned as above.

Dissemination, as outlined below, was made on dates indicated.

Pertinent information from above-referenced teletype.

Name and Location	Date Furnished
[redacted]	3/24/93

264A-SF-71590-2

b3
b6
b7C
b7D
b7E

~~SECRET~~

~~Classified by 0345~~
~~Declassify on OADR~~

2 - Bureau
2 - Canberra
(1 - 66-10)
(1 - [redacted]
(4) [redacted]

rec'd by [redacted]
2/26/93

[redacted]

4/26/93

~~SECRET~~

~~SECRET~~

b6
b7C

Memorandum

To : DIRECTOR, FBI

Date 4/16/93

From [redacted] CANBERRA [redacted]

b3
b6
b7C
b7E

Subject: [redacted]
NASA AMES RESEARCH CENTER - VICTIM;
COMPUTER FRAUD AND ABUSE IMPAIRMENT;
OO: SF

Reference: San Francisco teletype dated 4/12/93.

Dissemination, as outlined below, was made on dates indicated.

copies of

Pertinent information from above-referenced teletype.

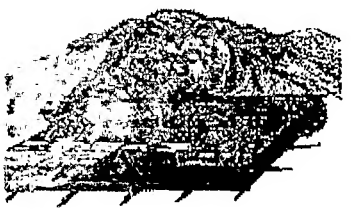
Name and Location	Date Furnished
[redacted]	4/16/93

264A-SF-97590-4

b3
b6
b7C
b7D
b7E

2 - Bureau
2 - Canberra
(1 - 66-10)
(1 - [redacted]
(4) [redacted]

b6
b7C



MAR 5 3 13 PM

FBI

SAN FRANCISCO DIVISION

PALO ALTO RESIDENT AGENCY

FAX: (415) 326-4975
Comm: (415) 326-4930

TO: SSA [redacted] X4566 Rm 4126

b6
b7C

RE: Per our Telcall - [redacted]

FROM: SA [redacted]

file copy

b6
b7C

AGENT COPY

0026 MRI 01026

PP FBISF

DE FBISF #0010 2821641

ZNR UUUUU

P 081636Z OCT 92

FM FBI SAN FRANCISCO ~~(264A-SF-97590)~~ (P) (PARA)

TO DIRECTOR FBI/PRIORITY/ [redacted]

b3
b7E

INFO FBI WMFO/PRIORITY/

BT

UNCLAS

CITE: //3790//

PASS: INTD, CI-2E, SSA [redacted]; WMFO, SSA [redacted],

b6
b7C

SA [redacted]

SUBJECT: "CHANGED" [redacted] NASA AMES RESEARCH CENTER-VICTIM; COMPUTER FRAUD & ABUSE-IMPAIRMENT; OO: SF.

RE SF AIRTEL (FD-801) AND ACCOMPANYING LHM DATED 2/27/92.

b6
b7C

TITLE MARKED "CHANGED" TO INCLUDE SUBJECT [redacted] IN THE CAPTION. TITLE FORMER CARRIED AS, "UNSUBS, [redacted] [redacted] NASA AMES RESEARCH CENTER-VICTIM; COMPUTER FRAUD &

File Copy

[redacted]

b6
b7C

Searched [redacted]
Serialized
Indexed
Filed

~~264A-SF-97590~~

ABUSE-IMPAIRMENT; OO: SF."

FOR INFORMATION OF LEGAT CANBERRA, IN NOVEMBER 1991, SYSTEMS ADMINISTRATOR FOR THE CRAY SUPERCOMPUTER AT THE NUMERICAL AERODYNAMIC SIMULATION (NAS) FACILITY AT NASA AMES RESEARCH CENTER (NARC), ADVISED THAT INTRUSIONS HAD BEEN MADE INTO THE "FRONT-END" COMPUTERS SUPPORTING THE CRAY. THE NAS IS DEVOTED TO RESEARCH ON CRITICAL TECHNOLOGIES, MAINLY IN THE AREA OF HIGH-MACH 3D WIND TUNNEL SIMULATIONS. THE SUBJECT GAINED ENTRY INTO THE NASA SYSTEMS, AND INSERTED A "TROJAN HORSE" PROGRAM. FROM THIS TROJAN HORSE, THE HACKER WAS ABLE TO BEGIN CRACKING PASSWORDS ON THE CRAY SYSTEM. AS A RESULT OF THIS ACTIVITY, NASA WAS FORCED TO SHUT DOWN THE FRONT-END COMPUTERS AT THE NAS FOR AN ENTIRE WEEK, WHILE SYSTEMS WERE RE-BOOTED AND RELOADED WITH CLEAN SYSTEM FILES. ADDITIONALLY, PASSWORDS ON THE SYSTEM HAD TO BE CHANGED. THE TOTAL LOSS WAS ESTIMATED AT BETWEEN 57,000 AND 500,000 DOLLARS, DEPENDING ON VALUATIONS OF SERVICES EXPENDED.

A REVIEW OF SYSTEM LOGS AND OTHER DOCUMENTATION SUPPLIED BY MR. [redacted] NAVAL RESEARCH LABORATORY (NRL), VIRGINIA, REVEALED A SYSTEMATIC SERIES OF ATTACKS ON NAS COMPUTERS BETWEEN OCTOBER 1991 AND DECEMBER 1991, EMANATING FROM HOST

b6
b7C

SITES IN AND AROUND SIDNEY, AUSTRALIA. THE MEDIUM OF ATTACK HAS BEEN INTRUSION AND MANIPULATION OF NAS FILES VIA THE INTERNET. THE INTERNET IS A VAST NETWORKING SYSTEM COMPRISED OF OVER 2000 SEPARATE COMPUTER NETWORKS WORLDWIDE, AND 8 MILLION KNOWN USERS. EACH SUB-NETWORK WITHIN THIS STRUCTURE SUPPORTS AN AVERAGE OF THIRTY COMPUTERS, SOME OF WHICH ARE DEDICATED TO ALL PHASES OF SCIENTIFIC RESEARCH. THE INTERNET IS FUNDED AND MAINTAINED BY THE U.S. GOVERNMENT.

IN JANUARY, 1992, [redacted] OF NRL FURNISHED [redacted] [redacted] WITH EXTENSIVE KEYSTROKE INFORMATION ON SUBJECT [redacted] TO DATE, THERE HAS BEEN NO RESPONSE FROM [redacted] WITH RESPECT TO [redacted] INVESTIGATION OF CAPTIONED MATTER. b6 b7C b7D

ON [redacted] AN ARTICLE APPEARED IN [redacted] [redacted] WITH A PICTURE OF [redacted], ALONG WITH EXTENSIVE INTERVIEW OF [redacted] DETAILING [redacted] [redacted] b6 b7C

LEAD

LEGAT CANBERRA

PAGE FOUR DE FBISF 0010 UNCLAS

AT MELBOURNE, AUSTRALIA: CONTACT [redacted] b6 b7C b7D

[redacted], AND DETERMINE

THE FOLLOWING:

[redacted] b6 b7C b7D b7E

BT

PAGE FIVE DE FBISF 0010 UNCLAS

#0010

NNNN

b6 b7C

[redacted]

ACTION COPY

0059 MRI 01781

PP FBISF

DE FBISF #0027 3292349

ZNY ~~SSSSS~~

P 12341Z NOV 92

[redacted] b3 b7E

FM FBI SAN FRANCISCO ~~(264A-SF-97590)~~ (P) (PARA)

TO DIRECTOR FBI/PRIORITY/

BT

~~S E C R E T~~

CITE: //3790//

PASS: INTD, CI-2E, SSA [redacted] b6 b7C

SUBJECT: [redacted] NASA AMES RESEARCH CENTER - VICTIM; COMPUTER FRAUD & ABUSE - IMPAIRMENT; OO: SF. b6 b7C

THIS ENTIRE COMMUNICATION IS CLASSIFIED ~~"SECRET"~~.

RE SF TT TO FBIHQ AND LEGAT CANBERRA DATED 10/7/92, CAPTIONED SAME.

File Copy

LEAD:

CANBERRA

AT SIDNEY:

SECURE COPY OF ARTICLE FROM [redacted] DATED

[redacted] b6 b7C

[redacted]

~~264A-SF-97590-37~~

PAGE TWO DE FBISF 0027 ~~S E C R E T~~

[redacted]

[redacted]. FORWARD COPY OF THIS ARTICLE, WITH PICTURE OF [redacted] TO SAN FRANCISCO.

b6
b7C

[redacted]

b6
b7C
b7D
b7E

SAN FRANCISCO REQUESTS LEGAT CANBERRA PROVIDE SAN FRANCISCO WITH AN UPDATE ON LEADS REQUESTED IN REFERENCED TT 10/7/92.

~~C/G-3;DCL/OADR.~~

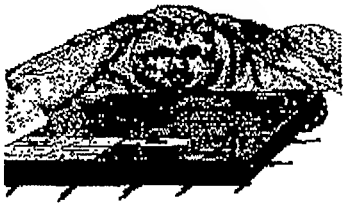
BT

#0027

NNNN

b6
b7C

358



FBI MAR 9 10 20 PM '93

SAN FRANCISCO DIVISION

PALO ALTO RESIDENT AGENCY

FAX: (415) 326-4975
Comm: (415) 326-4930

TO: SSA [redacted] x4566 Rm 1226

RE: Per our Telcall - [redacted]

FROM: SA [redacted]

b3
b6
b7C
b7E

[redacted] - per our telcall 3/9, the attached should round out your file. Any questions, give a holler. TX!

[redacted]

[redacted]

b6
b7C

264A-SF-97590/GZH Thu Jan 07 1993

Attached and incorporated herein is a fax from SA [redacted] WMFO, dated 1/7/93, encompassing a summary report by the Australian Embassy concerning [redacted] [redacted]

b6
b7C

Facsimile Coversheet

Washington Metropolitan Field Office
The National Computer Crimes Squad

To: FBI, SAN FRANCISCO, PALO ALTO RA Date: 1/7/93

Facsimile number: 415/326-4975

Attn: SA [redacted]

From: FBI, WMFO, NCMRA, C-17

Subject: [redacted]

[redacted]
b3
b6
b7C
b7E

file copy

Special Handling Instructions PLEASE HAND CARRY TO SA [redacted]
b6
b7C

No. of Pages (includes this sheet) 3

Originator's Name: SA [redacted]

Telephone: (202) 324-6360

Originator's Facsimile Number: (202) 324-6363

Approved: _____

S [redacted]

b6
b7C

EMBASSY OF AUSTRALIA

IN REPLY QUOTE: *6.91.158*

August 12, 1992

Special Agent [redacted] b6 b7C
Computer Crime Squad
Federal Bureau of Investigation
7799 Leesburg Pike
Suite 200 South
Falls Church, VA 22043

Dear [redacted]

COMPUTER HACKING

b7D

I have received a report from the [redacted] *in regard to the investigation of the activities of* [redacted] *The brief details are as follows.*

[redacted] b6 b7C b7D

[redacted] b7D

I will keep you advised of any developments in this matter which came to notice, but please do not hesitate to telephone me on [redacted] should you have any queries or should I be able to assist you in any way.

Yours sincerely

[redacted] b6 b7C

Assistant to the
Attache, Police Liaison
Washington DC

b6
b7C

264A-SF-97590/GZH

On 12/30/92 AUSA [redacted] advised that the key to whether captioned matter will be taken forward to prosecution hinges upon:

[redacted]

b5
b6
b7C
b7D

AUSA [redacted] indicated he will review the matter when pending lead requests have been covered, and information is obtained from [redacted]

b6
b7C

264A-SF-97590/GZH Thu Dec 17 1992

On 12/16/92 a copy of the Interim Prosecutive Report on captioned matter was forwarded to AUSA [redacted], Chief, DOJ Computer Crime Unit, pursuant to [redacted] request.

b6
b7C

COMPUTER FRAUD AND ABUSE DATA TRANSMITTAL FORM
FD-801 (11-6-91)

ALL FBI INFORMATION CONTAINED HEREIN IS UNCLASSIFIED DATE 03-24-2023 BY [redacted] b6 b7C

AIRTEL

To : Director, FBI
(Attn: Economic Crimes Unit
White-Collar Crimes Section
Criminal Investigative Division)

From : SAC, San Francisco [redacted] (P) b3 b7E

file copy

TITLE : Unsub(s) AKA [redacted] b6 b7C
NASA Ames
Research Center - VICTIM
COMPUTER FRAUD AND ABUSE - Impairment
CC: SF

REFERENCE: T/T From WMFO to HQ & SF dated 2/21/92

Check Box

☒ Enclosed are the original and five copies of a LHM for dissemination.

Check one

Submission: ☒ Initial ☐ Supplemental

1/27/92 Date case opened (if applicable) (As a 364. Formerly carried as [redacted] b3 b7E

__/__/__ Date of complaint

10/11/91 Date of first known offense/intrusion

200 - Estimated number of computer users affected.

$ 500,000 - Estimated loss to date.

Sun Workstations Brand and series model of computer (ie: IBM, DEC, Apple, etc.)

Unix Operating system and version.

[redacted] b6 b7C

3 - Bureau
(1 - ECU, WCCS, CID)
(1 - CI-4D, INTD)
2 - Field Office

FBI/DOJ

CC

Fill in below with Yes (Y), No (N), or Unknown (U):

Y Is a federal government computer affected?
Department/Agency: NASA

Y Is a federal interest computer affected?
Victim institution: Stanford

Y Does the offense involve a telecommunications network?
N Is (former) employee suspected?
Y Is the method of intrusion known?
Y Is the system still vulnerable?
Y Is the intrusion continuing? (Door Rattling)

National Security Issues:

Y Does agency/institution computers contain classified information?
U Was classified information compromised in this matter?
U Is a foreign or hostile intelligence service involved?

Check Type Of Crime(s):

IMPAIRMENT (264-A)

- ☐ Virus Planted
- ☐ Malicious Software Planted
- ☒ Interruption of Service/Prevent use
- ☐ Destruction of Information or Software
- ☒ Modification of Information or Software

THEFT OF INFORMATION (264-B)

- ☒ Data
- ☒ Passwords
- ☒ Computer Processing Time
- ☐ Telephone Services
- ☐ Application Software
- ☐ Operationg System Software

INTRUSION (264-C)

- ☐ Unauthorized Access
- ☐ Exceeding Authorized Access

Check Action Taken:

- ☒ Case Opened/Reopened/Incorporated into Pending Matter
- ☐ No Action Due to State/Local Prosecution
- ☐ USA Declination
- ☐ Facts Known do not meet Prosecutive Guidelines
- ☐ Matter Referred to Another Federal Agency (U.S. Secret Service)
- ☐ Investigation Delayed Due to Lack of Resources
- ☐ Other: _____

Administrative:

U.S. Department of Justice
Federal Bureau of Investigation

San Francisco, California — February 27, 1992

UNSUB(S), AKA
[redacted]

NASA AMES RESEARCH CENTER- VICTIM;
COMPUTER FRAUD AND ABUSE- IMPAIRMENT;
OO: SAN FRANCISCO

b6
b7C

PREDICATION:

In November 1991, a systems administrator for the Cray Supercomputer at the Numerical Aerodynamic Simulation (NAS) Facility at NASA Ames Research Center, advised that intrusions had been made into "front-end" computers supporting the Cray. The NAS is devoted to research on critical technologies, mainly in the area of high-mach 3D wind tunnel simulations. The hacker(s) gained entry via a Thinking Machines, Sun work station (tmc.sun), inserted a trojan horse program, and began cracking passwords. As a result of this activity, NASA was forced to shut down the front-end computers at the NAS for a week, while systems were re-booted and re-loaded with clean system files. Additionally, all passwords on the system had to be changed. The total loss was estimated at between $57,000 and $500,000, depending on valuation of services expended. The lower figure represents in-house costs, while the latter reflects the value of corrective work based on a service contracted to an outside source. This constitutes a violation of 18 USC §1030, which the Northern District of California U.S. Attorney's Office has agreed to consider for prosecution.

INVESTIGATION

This case is being investigated by the FBI and the NASA Inspector General's Office (NASA/IG).

A review of system logs and keystroking documentation supplied by Naval Research Laboratory (NRL) Virginia, has revealed a systematic series of attacks on NAS computers between October 1991 and December 1991, emanating from host sites in and around Sydney Australia. The medium of attack has been intrusion and manipulation via the Internet (See chart of hacking activity attached hereto). The Internet is a vast networking system encompassing over 2,000 separate computer networks worldwide. Each sub-network within this structure supports an average of 30 computers, dedicated to all phases of scientific research. It is funded and maintained by the U.S. Government. As a network linking high-performance computers and leading edge networking, data storage, and software development technologies, Internet is defined as a "core technology" within gui[redacted] ies set forth by the National Critical Technologies Panel,

b7E Per NASA
b6
b7C

[redacted]